Ein Verlagsbeihefter der Heise Zeitschriften Verlag GmbH & Co. KG



Security

Schwerpunkt: Unified Threat Management

Veranstaltungen

26. – 30. Oktober, Dubai
RIPE 57
www.ripe.net/ripe/meetings/ripe-57

9. – 11. Februar 2009, Hamburg
4. – 6. März 2009, Frankfurt/Main
18. – 20. März 2009, Stuttgart
7. – 29. Mai 2009, Wien
Kerberos – LDAP – Active Directory
www.ix-konferenz.de

iX extra Security zum Nachschlagen:
www.heise.de/ix/extra/security.shtml

Weniger ist mehr

Die Wahl des maßgeschneiderten Systems

Aus rechtlicher und wirtschaftlicher Sicht ist die Bereitstellung von Sicherheitsdiensten für ein Unternehmen nahezu zwingend. Doch bei der Wahl eines Rundum-Sorglos-Pakets wie Unified Threat Management (UTM) sollten Betriebe sich genau überlegen, welche Dienste sie wirklich benötigen.

Unter dem Namen Unified Threat Management (UTM) haben sich Rundum-Sorglos-Sicherheitspakete etabliert. Dies gilt zumindest für den Bereich, der das interne Netz von der Außenwelt oder auch zwei Netze voneinander trennt. Ursprünglich beschrieb diese Gattung lediglich ein Produkt, das Firewalls, IDS/IPS (Intrusion Detection System, Intrusion Prevention System) und Anti-Virus in einer Lösung vereinte. In der Zwischenzeit gibt es kaum noch einen Anbieter, der sich auf diese Minimalanforderungen beschränkt. Je nach Hersteller gelangten weitere Funktionen in die jeweiligen Appliances, von Virtual Private Networks (VPNs) über URL- und Content-Filtering-Funktionen, die Absicherung von Social-Networking-Plattformen bis zur Sicherstellung von Quality-of-Service- Anforderungen im Voice-over-IP-Bereich.

Leider gilt die Definition von UTM nicht mehr für die heutigen Gegebenheiten. So kocht mittlerweile jeder Hersteller sein eigenes UTM-Süppchen mit verschiedenen Zutaten, was einen Vergleich zwischen den einzelnen Produkten deutlich erschwert, da sie mit unterschiedlichen Diensten ausgestattet sind.

Unternehmen sollten sich daher die Frage stellen, welche Dienste zum Schutz der Organisation wirklich unbedingt erforderlich sind. Selbstverständlich hat hier jeder Sicherheitsexperte und natürlich der jeweilige Produkthersteller eine eigene Meinung. Allerdings existieren einige rechtliche und auch wirtschaftliche Aspekte, die die Bereitstellung von bestimmten Sicherheitsdiensten für ein Unternehmen fast schon zwingend erforderlich machen. Dass hierbei eine Firewall als zentrales Ein- und Ausgangstor in angrenzende Netze als absolut notwendig gilt, dürfte wohl niemanden verwundern.

Vor dem Kauf eines UTM-Produkts sollten sich die Verantwortlichen überlegen, ob eine einfache Firewall ausreicht, die ein- und ausgehende Datenpakete mithilfe der sogenannten Stateful Inspection überprüft, oder ob der Einsatz von Proxies für dedizierte Protokolle sinnvoller ist. So haben etliche Hersteller in ihre UTM-Firewalls Pro-

xies für SIP, H323, NetBIOS, VNC (Virtual Network Computing), RTP (Realtime Transport Protocol), DNS (Domain Name System) und so weiter integriert. Ebenso zwingend notwendig wie eine Firewall ist die Installation eines Anti-Virus-Gateways für die Überprüfung ein- und ausgehender Datenströme. So werden die eigenen Daten vor entsprechenden Schädlingen und dadurch vor einem eventuellen Vernichten, Verändern oder Ausspähen geschützt. Darüber hinaus lässt sich so das Risiko reduzieren, selbst Viren zu verbreiten. Trägt das eigene Unternehmen an der Verbreitung von Viren eine Mit- oder gar Hauptschuld und haben andere dadurch einen Schaden erlitten (etwa einen Datenverlust), so kann es durchaus dazu kommen, dass der Haftungsfall eintritt.

Sind innerhalb des Unternehmens Mitarbeiter oder Auszubildende beschäftigt, die unter 18 Jahre alt sind, so gelten diese als Schutzbefohlene. Der Arbeitgeber muss also unter anderem sicherstellen, dass diese im Internet nur die für sie geeigneten Inhalte einsehen können.

Dies versuchen Unternehmen im Allgemeinen mittels eines URL- oder Web-Content-Filters sicherzustellen. Der freie Zugang zum Internet für diesen jugendlichen Personenkreis könnte ebenfalls rechtliche Konsequenzen haben. Abgesehen davon kann der Aufruf von bestimmten Internetseiten auch für Erwachsene persönlichkeitsverletzend sein und sollte schon aus diesem Grund unterbunden werden. Bei der Auswahl des richtigen UTM-Systems sollte man deshalb auch diese Anforderung berücksichtigen.

Altersgerechter Schutz

Aber dies sind natürlich nicht alle Aspekte, die aktuelle UTM-Produkte abdecken. Sollen zum Beispiel Mitarbeiter von unterwegs oder daheim auf interne Daten zugreifen können, ist der Aufbau von verschlüsselten Verbindungen eine zwingende Anforderung (VPN-Access-Point). Dafür gibt es verschiedene Möglichkeiten. Sollen einem Nutzer bei einem Zugriff von außen lediglich dedizierte Anwendungen zur Verfügung stehen, wäre der Einsatz eines SSL-VPNs anzuraten, das ihm genau diese Anwendungen über eine entsprechende Oberfläche zur Verfügung stellt. Soll sich der Nutzer bei einem Zugriff von außen genau so wie an seinem internen Arbeitsplatz fühlen, wäre der Einsatz von VPNs via IPSec sicherlich eine gute Wahl. Dies gilt auch, wenn verschiedene Standorte über das Internet miteinander verbunden werden sollen (Site-to-Site VPN). Leider bieten nicht alle UTM-Appliances beide Möglichkeiten.

Generell ist natürlich auch die Frage wichtig, welche Dienste Daten über das UTM-System übertragen sollen. Hierbei sind vor allem zeitabhängige Anwendungen zu beachten. Voice over IP ist nur ein Beispiel eines in dieser Hinsicht kritischen Dienstes. In einem solchen Fall sollten Verantwortliche bei der Auswahl eines UTM-Produkts auch prüfen, ob es in der Lage ist, Quality-of-Service-Funktionen umzusetzen. Anderenfalls kann es passieren, dass bei größeren Datentransfers zwischen den jeweiligen Endpunkten die Leitung so stark belegt wird, dass ein Telefonat zwischen den beiden Standorten nicht mehr möglich ist.

Neben der Fähigkeit der Integration von Quality-of-Service-Funktionen sind etliche der aktuellen UTM-Systeme in der Lage, mit Virtual LANs (VLANs) umzugehen. Dies kann sich insbesondere dann als kritische Funktion entpuppen, wenn das System im internen Netz eingesetzt werden soll, zum Beispiel zur Abtrennung verschiedener interner Teilnetze. Nahezu jede UTM-Appliance besitzt, wie in der ursprünglichen Definition vorgesehen, ein Intrusion-Detection- beziehungsweise Intrusion-Protection-Subsystem. Dies kann, sofern sauber konfiguriert und integriert, wichtige Erkenntnisse über das Risiko in dem betrachteten Netz liefern. Allerdings ist der Aufwand für die Konfiguration eines solchen Systems deutlich höher als bei den anderen Subsystemen wie Firewall oder Anti-Virus. Mit einer guten Konfiguration können IT-Fachleute jedoch Kennzahlen gewinnen, die als Argumentationshilfen für zukünftige Security-Projekte innerhalb des Unternehmens dienen können.

Die relativ große Anzahl von UTM-Anbietern hat zu einer großen Bandbreite an Einzelsystemen geführt. Für nahezu jedes Unternehmen ist etwas dabei. Günstige kleine Systeme, die sich etwa zur Absicherung und Anbindung von kleineren Außenstellen eignen, sind genauso anzutreffen wie teure Produkte, die sich gut im Backbone eines größeren Unternehmens einsetzen lassen. Die Performance der Systeme hängt dabei in einem hohen Maße von den aktivierten Diensten ab. Dies gilt insbesondere für rechenintensive Bereiche wie die

ANBIETER VON UTM-PRODUKTEN

Die Übersicht erhebt keinen Anspruch auf Vollständigkeit.

Hersteller	Produkt	Webadresse
Astaro	ASG 110/120	www.astaro.com
Check Point	UTM-1	www.checkpoint.com
Collax	Security Gateway	www.collax.com
Computer Associates	HIPS 8.0	www.ca.com
Fortinet	Fortigate	www.fortinet.com
Funkwerk	Funkwerk UTM	www.funkwerk-ec.com
Gateprotect	GPO	www.gateprotect.de
IBM	Proventia	www.iss.net
Juniper Networks	SSG (verschiedene)	www.juniper.net
NetASQ	F50	www.netasq.com
Phion	netfence M3	www.phion.com
Secure Computing	Sidewinder G2	www.securecomputing.com
Securepoint	Piranja	www.securepoint.de
Smoothwall	Smoothguard 1000 UTM	www.smoothwall.net
SonicWall	NSA E7500 / PRO 3060	www.sonicwall.com
Symantec	Endpoint Protection	www.symantec.com
Telco Tech	LiSS xxx series	www.telco-tech.de
Underground_8	Limes MF	www.underground8.com
Vasco	aXs Guard	www.vasco.com
Watchguard	Firebox X Edge/Core/Peak	www.watchguard.de

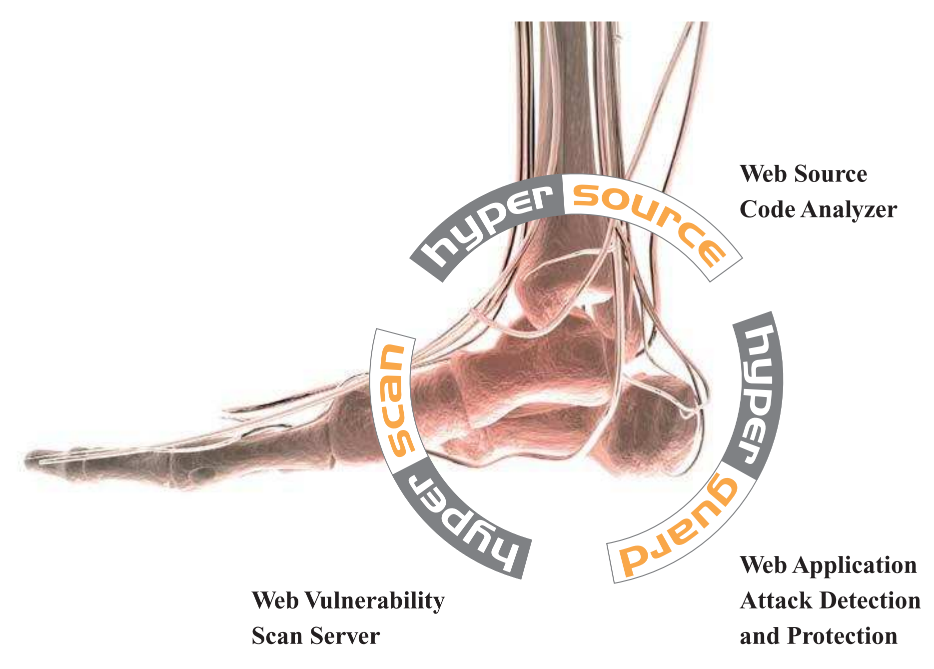
Anzeige

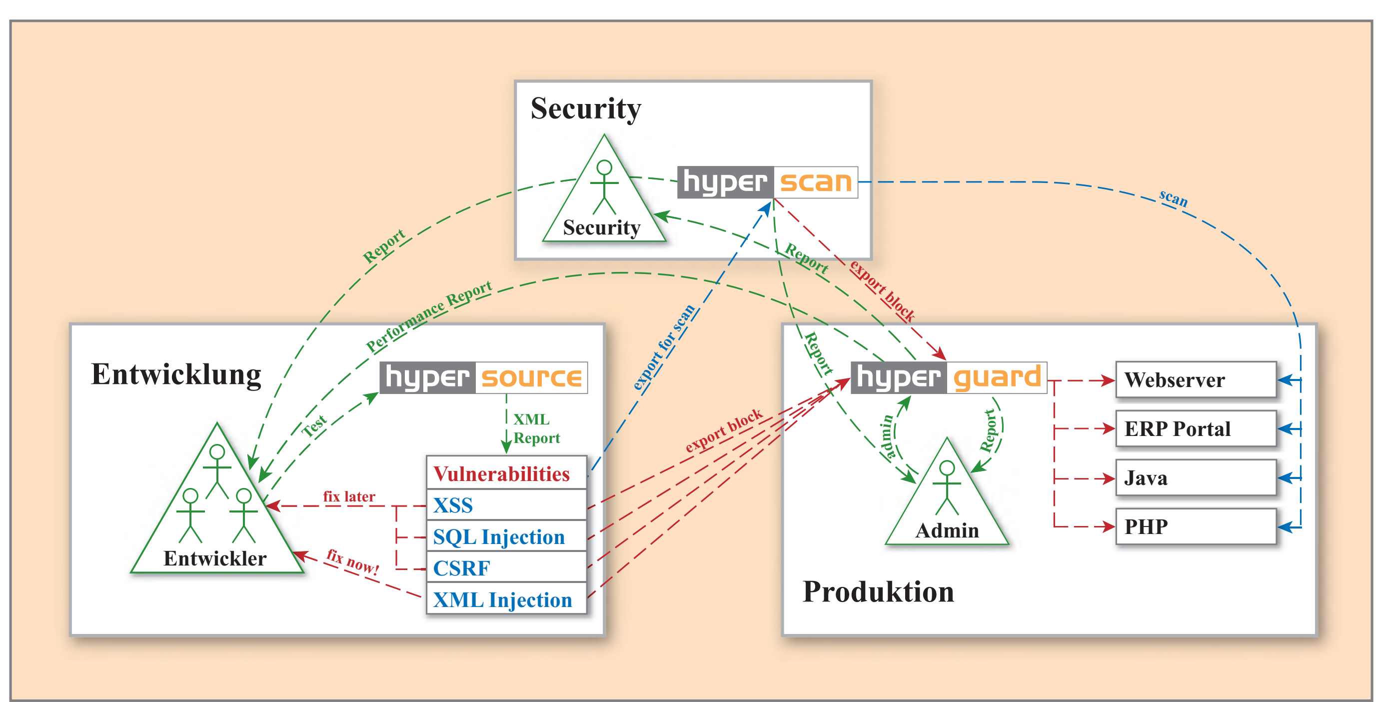
Achillesferse Web-Applikation

art of defence, Softwarehersteller aus Regensburg, bietet die derzeit umfassendste Produktpalette im Bereich Web Application Security.
Schwachstellen im Web Source Code werden vom Analysetool hypersource identifiziert. Dabei werden alle Entry-Points der Reihe nach überprüft und mittels Data-Flow-Analyse komplett bis zum ‘Exit’ verfolgt. So werden alle Verwundbarkeiten bis zu ihrer Wurzel aufgezeigt.
Der Web Vulnerability Scan Server hyperscan überprüft Websites mit unterschiedlichen Techniken von außen. Ein intelligenter Crawl-Mechanismus arbeitet sich durch die erreichbaren Links und penetriert die Applikation u.a. mit Signaturen aus seiner Datenbank. Einzigartig ist hier das Zusammenspiel mit dem Source Code Analyzer hypersource: Die gefundenen Schwachstellen können von hyperscan importiert werden, um die Filtermechanismen der Applikation zu überprüfen.
Die Web Application Attack Detection übernimmt hyperguard von art of defence. Als Plug-In in Webserver und viele andere Infrastruktur-Produkte kann hyperguard überall verteilt werden.

Eine zentrale Managementkonsole bietet ausführliches Monitoring, Reporting und Alerting sowie aktuelle Statusreports über die Applikationssicherheit.
Zudem ist hyperguard mit einer sehr ausgereiften Protection-Funktionalität erweiterbar: Damit können u.a. ältere Applikationen sehr einfach mit einem Grundschutz versehen oder komplexe Portallösungen in ihrem externen Verhalten abgesichert werden.

Ein Novum in diesem Bereich ist der automatische Regelvorschlag von hyperguard durch den Import von Schwachstellen der Source Code Analyse und von aufgedeckten Lücken des Scan Servers. Alle Produkte bieten ein ausführliches Reporting z.B. nach den bekannten OWASP-, CWE- oder PCI-Richtlinien und dienen so zum Nachweis der Einhaltung rechtlicher Vorschriften und Industrie-Standards.





Zusammenspiel und Einsatz der Produkte

www.artofdefence.com

Verschlüsselung oder den Einsatz von Virenscannern. Da keine verbindlichen Vorgaben existieren, wie Hersteller die Performance ihrer Systeme messen sollten, ist ein Vergleich der Lösungen anhand der nackten Zahlen auf den Datenblättern wenig sinnvoll. Grundsätzlich gilt es zu prüfen, mit welchen Daten und mit welchen aktivierten Diensten ein solcher Test lief, damit wirklich ein Urteil über die Leistungsfähigkeit eines Systems möglich ist. Ob die Performance ausreicht, ist letzten Endes nur mittels eines Tests mit eigenen Testdaten herauszufinden.

Cluster und die Performance

Etliche Hersteller ermöglichen es, einzelne Systeme zu Clustern zusammenzufassen und damit die Performance zu erhöhen. Ein nützliches Merkmal, da auf diese Weise das Sicherheitspaket mit dem Wachstum eines Unternehmens Schritt halten kann. Auch ergibt sich so die Möglichkeit, ein System zu erweitern, insbesondere wenn zum Beispiel zusätzliche Dienste auf dem System aktiviert werden müssen, deren Einsatz im Vorfeld nicht abzusehen war.

Neben der Performance erhöht ein Clustering von Systemen auch die Ausfallsicherheit. Diese ist allerdings nur dann gewährleistet, wenn die nach einem Ausfall verbliebenen Systeme die anfallende Last auch bearbeiten können.

Um die Verfügbarkeit der Dienste zu gewährleisten, ist ein Clustering nicht unbedingt notwendig. Hier reicht bereits eine Standby-Lösung, die nahezu alle größeren Pakete bieten. Es stellt sich lediglich die Frage, ob eine Cold-Standby-Lösung ausreicht oder ob eine Hot-Standby-Lösung notwendig ist. Bei einer Cold-Standby-Lösung wird das Ersatzsystem erst aktiviert, wenn das ursprüngliche System ausgefallen ist. Bestehende Verbindungen müssen dann neu aufgebaut werden, was nicht bei jeder Anwendung machbar ist. VPN-Nutzer müssten beispielsweise einen neuen Tunnel aufbauen, da das Ersatzsystem nichts davon „weiß“, dass sie bereits mit dem internen Netzwerk verbunden waren. Bei einer Hot-Standby-Lösung erhält das Ersatzsystem grundsätzlich dieselben Informationen wie das aktive System. Bei einem Ausfall kann es so alle offenen Verbindungen übernehmen. Die darüber laufenden Dienste bemerken also den Ausfall gar nicht. Ob Clustering, Hot- oder Cold-Standby die beste Lösung darstellen, ist meistens auch eine Frage des zur Verfügung stehenden Budgets.

Um Systeme im Nachhinein performanter zu betreiben, bieten manche Hersteller Erweiterungen durch Ko- oder Kryptoprozessoren an. Dies ist insbesondere dann sinnvoll, wenn die innerhalb einer UTM-Appliance vorhandenen rechenintensiven Dienste wie VPN stark in Anspruch genommen werden. Hier lässt sich unter Umständen einiges an Geld sparen, da der Nachkauf einer solchen Karte deutlich günstiger ist als das Auswechseln eines ganzen Systems.

Außerdem kann die Reihenfolge, in der die Dienste inner-

halb des UTM-Geräts den Datenstrom abarbeiten, die Performance beeinflussen. Die Reihenfolge Firewall, IPS und Anti-Virus ist im Allgemeinen weniger rechenintensiv als umgekehrt, weil im ersten Fall schon ein Großteil des Datenstroms gefiltert wird und gar nicht erst zur weiteren Verarbeitung an die Folgesysteme gelangt. Bei den meisten UTM-Systemen ist jedoch die Reihenfolge, in der die einzelnen Services die Daten überprüfen, fest vorgegeben. Nur ganz wenige Hersteller bieten den Luxus einer freien Konfiguration. Dabei kann es durchaus interessant sein, ein IPS/IDS direkt an der Internetschnittstelle (Perimeter) lauschen zu lassen und so ein Gefühl dafür zu bekommen, wie vielen Angriffen das eigene Netzwerk denn tatsächlich ausgesetzt ist.

Neben den reinen Konfigurationsmöglichkeiten ist die Managementschnittstelle von wesentlicher Bedeutung. Die Definition von Rollen und die Zuweisung von Accounts zu diesen Rollen beherrschen nahezu alle größeren und meist auch kleineren Systeme. Zumindest erlauben sie den (lesenden oder schreibenden) Zugriff auf die einzelnen Konfigurationen. Das Ausblenden von bestimmten Bereichen für manche Rollen (zum Beispiel darf der Anti-Viren-Admin keine Einsicht in das Firewall-Regelwerk nehmen) beherrschen ebenfalls einige der teureren Systeme. Solche Möglichkeiten werden vor allem für den Einsatz in Großunternehmen benötigt, wenn sich unterschiedliche Gruppen um unterschiedliche Bereiche kümmern müssen. Die Integration des Systems in eine zentrale Benutzerverwaltung via LDAP (Lightweight Directory Access Protocol), Active Directory oder ähnliche Dienste ist jedoch für nahezu jeden Kunden interessant, und daher bieten viele Systeme diese Funktionen an.

Setzen Unternehmen mehrere UTM-Systeme in einem Netz ein, ist eine zentrale Verwaltung für Policies, Firewalls, IDS/IPS und Virenscanner unbedingt erforderlich, um den Aufwand in Grenzen zu halten. Auch das Verteilen von Patches für die eingesetzten Appliances ist über eine solche Umgebung deutlich einfacher als bei einer dezentralen Verwaltung. Zum Teil müssen Anwender dafür ein entsprechendes Management-Center erwerben, was zusätzliche Kosten verursacht. Diese Managementumgebungen erlauben es auch, die Protokollierungsmöglichkeiten der einzelnen Systeme und der auf den Systemen laufenden Services in einer zentralen Umgebung zusammenzufassen.

Allerdings beherrschen die wenigsten Produkte eine richtige Event-Korrelation. Hier werden Anwender in den meisten Fällen nicht um eine zusätzliche Anschaffung herumkommen. Die Konfiguration von Alarmen hingegen ist mit nahezu jedem System möglich. Dabei verschicken die Systeme meistens bei einer vorher zu definierenden Log-Nachricht einen SNMP-Trap, eine E-Mail oder Ähnliches an einen festgelegten Empfänger. Manche Hersteller liefern sogar die Möglichkeit, Schwellwerte zu definieren, ab denen ein solcher Alarm ausgelöst wird.

Fazit

UTM-Produkte sind heutzutage ein wesentlicher Teil des Security-Alltags, und dies nicht nur wegen des meist guten Kosten-Nutzen-Verhältnisses. Die Administration sämtlicher Security-Dienste über eine dedizierte Benutzerschnittstelle gefällt vielen Administratoren und verspricht eine kürzere Einarbeitungsphase. Die nötige Schulung lässt sich aber nicht in zwei bis drei Tagen erledigen. *Jörn Maier*

Kontrollierter Wiedereintritt

Network Admission Control als moderne Netzzugangssicherung

Network Admission Control (NAC) hat auf den ersten Blick alles, was einen typischen IT-Hype ausmacht: Der Begriff ist erst seit gut zwei Jahren in der Diskussion, wird von IT-Sicherheitsanbietern gepusht und vereint technisch gesehen nur altbekannte Sicherheitstechniken zu einem neuen Modell. Doch der Eindruck täuscht.

Auch wenn viele angesichts immer neuer Modebegriffe nur noch gelangweilt abwinken – Network Admission Control (NAC) ist mehr als ein Marketingschlagwort. Hinter NAC steckt ein sinnvolles Konzept, das auf die zunehmende Mobilität von Unternehmensmitarbeitern reagiert.

Ziel der NAC-Technik ist es, Netzwerksicherheit auch dann zu gewährleisten, wenn sich Geräte von Netzteilnehmern zeitweise außerhalb eines Unternehmensnetzes, seiner Sicherheitssysteme und der Kontrollmechanismen für seine Policies befinden. Viren, Trojaner oder Spyware, die in einer fremden Umgebung auf den PC eines Mitarbeiters geraten sind, können beim nächsten Kontakt des Geräts mit dem internen Netz überspringen. Zumindest gilt dies, wenn die Schutzsysteme des internen Netzes dem „eigenen“ Computer einfach vertrauen und Daten vom Firmen-PC ungeprüft durchlassen. NAC unterwirft deshalb alle Geräte, die sich mit einem Netz verbinden wollen, zunächst einer Kontrolle und stellt fest, ob sie für eine uneingeschränkte Verbindung noch sicher genug sind oder erst einer Spezialbehandlung unterzogen werden müssen.

Diese Grundidee, ihr Wert und die einzelnen NAC-Spielarten lassen sich am besten bewerten, indem man einen Blick auf frühere Lösungsansätze für die Mobilproblematik und ihre Limitationen wirft.

Das Ende des geschlossenen Netzes

Anfangs war es ein unausgesprochenes Ziel der Administration, den Zustand eines geschlossenen Netzes so weit wie möglich zu erhalten. Der externe Mitarbeiter wurde über direkte Modemeinwahl und später über eine VPN-Leitung erst authentifiziert und dann wie mit einem verlängerten Kabel wieder „ins Netz geholt“. Dort schützte die Unternehmens-Firewall sein Gerät wie einen echten internen PC und hielt es im Zugriffsbereich des Administrators. Den Internetzugang gewährte man in einem solchen Fall folgerichtig über den Umweg des Unternehmensnetzes, um hier alle Filter und Schutzmechanismen des Gateways wirken zu lassen.

Dies kann als der erste Lösungsversuch für das Problem der zunehmenden Mobilität der Arbeitsplatz-PCs gesehen werden. In Unternehmen, die so vorgehen, sind die Sicherheitsmaßnahmen noch immer auf ein Arbeitsplatzkonzept zugeschnitten, das den per Kabel angeschlossenen und permanent kontrollierbaren PC als Normalfall betrachtet. Funktionieren kann das Konzept in Organisationen, die ihren reisenden Angestellten überall rund um die Uhr schnelle VPN-Gateways zur Verfügung stellen können.

Jenseits des VPN

In den meisten Fällen allerdings nutzen und benötigen Mitarbeiter Zugriff aufs Internet auch unabhängig von VPN-Verbindungen ins Unternehmensnetz. Die Internet-Zugriffsrichtlinien, die im internen Netz eines Unternehmens zum Beispiel durch die Blockade bestimmter Webseiten am Gateway kontrolliert werden können, gelten aber weder zu Hause noch in Hotels, an Flughäfen und in öffentlichen Cafés. Dies und die fehlenden Gateway-Filter erhöhen die schon beschriebene Gefahr, dass Malware auf den Rechner gelangt – etwa, wenn der Anwender bewusst fremde Software auf seinen Rechner lädt, wenn er auf einer scheinbar harmlosen Seite im Internet in eine Download-Falle gerät oder wenn er eine ungeschützte E-Mail-Verbindung nutzt. Möglicherweise ist auch bereits das fremde Netz kompromittiert, über das er sich Verbindung zum Internet verschafft. Zweifellos helfen gegen solche Gefahren autonome Sicherheitspakete für Clients, aber es gibt keine Garantie, dass diese permanent funktionieren und dass sie der Anwender nicht einfach außer Betrieb setzt, wenn sie stören.

Ein zweiter Lösungsweg setzt hier an und unternimmt den Versuch, Zugriffs- und Sicherheitsrichtlinien unabhängig vom Gateway fest im mobilen Rechner zu verankern. Das Gerät wird dazu mit Sicherheitssoftware ausgestattet, die sich nicht vom Anwender umkonfigurieren lässt und die gleichen Restriktionen durchsetzt wie im heimischen Netz. Dieses Konzept aber wirft eigene Probleme auf: Zu oft erfordern es die Umstände auf Reisen, dass der Anwender eben doch Änderungen vornehmen muss, um überhaupt eine Verbindung aufnehmen zu können – und dann hat er keine Chance, wenn die Sicherheitssoftware für ihn gesperrt und der Administrator nicht rund um die Uhr erreichbar ist. Außerdem gibt es Geräteklassen wie bestimmte Smartphones und PDAs oder auch technische Spezialgeräte, die nicht ohne Weiteres das Installieren geeigneter Client-Software zulassen.

Gäste als Sicherheitslücke

Noch komplizierter wird die Situation durch die neuesten Trends der modernen Arbeitswelt. Externe Berater, Zeitarbeitskräfte und auf freier Basis verpflichtete Mitarbeiter übernehmen in immer mehr Organisationen Aufgaben, die früher fest angestellten Mitarbeitern vorbehalten waren. Die „Freien“ arbeiten mit eigenen Rechnern, über die der Unternehmensadministrator keine Kontrolle hat, erwarten aber selbstverständlich an ihrem Einsatzort Zugriff aufs Internet, aufs eigene Mail-System und auf ausgewählte Ressourcen des Kunden. Auch auf solche Konstellationen muss ein modernes Netz reagieren können.

Network Admission Control oder Network Access Control, manchmal auch Network Access Protection (NAP), ist tatsächlich die bisher ausgefeilteste Antwort auf die beschriebenen Probleme. NAC lässt mobile Geräte temporär frei, unterwirft sie beim erneuten Kontakt mit dem Unterneh-

mensnetz aber wieder dessen Regeln. Geräte, die sich mit einem Netzwerk verbinden, werden dazu auf mehreren Ebenen geprüft:

– Ist der Anwender bekannt?
– Ist sein Gerät bekannt und registriert?
– In welchem Sicherheitszustand befindet sich das Gerät, und entspricht er den Regeln des Unternehmens?

Die möglichen Antworten auf die letzte Frage betreffen die sogenannte Endpoint Security und umfassen Informationen wie die installierte Software, den Aktivitätszustand von Virenschutz, Firewall und anderen Sicherheitswerkzeugen und den Patch-Stand der System-, Anwendungs- und Sicherheitssoftware mit den jeweiligen Signaturdateien.

Auf die Ergebnisse muss das Netz möglichst fein abgestuft reagieren können. Fremdrechner beispielsweise könnte es in ein separates Gästenetz eingliedern, etwa ein virtuelles LAN (VLAN), das nur Internet- und Mail-Zugang bietet. Hier kann der Administrator dem Gast dann einzelne interne Ressourcen gezielt zuteilen. Noch radikalere Lösungen weisen dem Gast nur eine virtuelle Weboberfläche als Arbeitsumgebung zu.

Die Verpflichtung zum „sauberen“ PC

Bekannte Rechner von bekannten Mitarbeitern können vollständig eingebunden werden, wenn ihre Schutzsysteme auf dem neuesten Stand sind und keine unbekannte Software installiert ist. Fehlen Patches oder weicht der Computerzustand aus anderen Gründen vom Soll ab, ist eine komplette Sperrung möglich. Eine Alternative bietet die temporäre Überführung in ein Quarantäne- und „Remediation“-Netz, das zunächst die verpassten Updates erzwingt und während der möglichst kurzen und transparenten „Reparatur“ des Computers keine oder nur wenige weitere Aktionen zulässt.

NAC hat eine Reihe verschiedener technischer Komponenten: Module, die das Gerät des Mitarbeiters erkennen und seinen Zustand bestimmen, Systeme, die die adäquate Behandlung des Geräts im Netz erledigen und Vorrichtungen, die die Unternehmensrichtlinien beim Wiedereintritt ins Netz erneut auf dem Endgerät selbst durchsetzen.

Bei der Authentifizierung des Geräts greifen Anbieter mehr und mehr auf Verfahren auf Basis des Layer-2-Protokolls 802.1X zurück. Bei Geräten, die nicht 802.1X-fähig sind, wird die MAC-Adresse genutzt. Bei internen Geräten kann das NAC-System vom Unternehmens-Directory erfahren, um welches System es sich handelt und ob dieses seinen Sicherheitszustand überhaupt ändern kann: Manche mobilen Maschinen oder Messgeräte etwa können zwar IP- und MAC-Adressen haben, sind aber fremder Software und damit auch Malware gar nicht zugänglich. Das Unternehmens-Directory oder ein Policy-Server geben Auskunft darüber, welche Regeln für ein Gerät unter welchen Umständen gelten. Völlig fremde Systeme, für die es keine Einträge in den Unternehmens-Repositories gibt, können ins erwähnte Gästenetz geschickt werden – wobei noch die Möglichkeit besteht, sie gesondert zu behandeln, wenn zumindest der Anwender bekannt ist.

ANBIETER VON NETWORK ADMISSION CONTROL

Die Übersicht erhebt keinen Anspruch auf Vollständigkeit.

Anbieter	Produkt	Webadresse
Bradford Networks	NAC Director Guest/ Contractor Services	www.bradfordnetworks.com
Check Point	Endpoint Security	www.checkpoint.com
Cisco	NAC	www.cisco.com
CoSoSys	Endpoint Protector	www.cososys.de
eEye Digital Security	Blink Professional	www.eeye.com
Enterasys	Enterasys Network Access Control	www.enterasys.com
Forescout	Counter Act	www.forescout.com
GFi	EndPointSecurity	www.gfi.com
HP	ProCurve NAC Endpoint Integrity	h40060.www4.hp.com
IBM	Proventia Desktop	www-935.ibm.com
ID Engines	Ignition	idengines.com
Impulse Point	Safe Connect	www.impulse.com
Insightix	NAC	www.insightix.com
Integrasul	NAC	nac.integrasul.inf.br
Juniper	Access Control Solutions	www.juniper.net
Kaspersky	Open Space Security	www.kaspersky.com/de
Lumension	Sanctuary	www.lumension.com
McAfee	NAC	www.mcafee.com/us
Mikado	Macmon	www.mikado.de
Mirage Networks	NAC	www.miragenetworks.com
NCP	Next Generation Network Access Technology	www.ncp.de
Neo Accel	Neo Accel NAC-Plus	www.neoaccel.com
Netclarity	NACwalls	www.netclarity.net
Nortel	SNAS	products.nortel.com
PGP	Endpoint	www.pgp.com/de
Prosoft	Safend Protector	www.prosoft.de
Secude	Finally Secure	www.secude.com
Sophos	NAC	www.sophos.de
Still Secure	Safe Access	www.stillsecure.com
Symantec	NAC	www.symantec.com/de
Tipping Point	Network Access Control	tippingpoint.com
Trend Micro	Viruswall Enforcer	www.de.trendmicro.com
United Security Providers	USP Network Authentication System	www.united-security-providers.com
Utimaco	SafeGuard	www.utimaco.de



Klare Vorteile für KMUs, Konzerne und Service Provider

Managed Security Services

Der Markt für Managed Security Services wächst beständig, jedoch galt es als schwierig und kostenintensiv, diese Dienstleistung im Outsourcing-Verfahren zu erbringen. Clavisters neue Security Service-Plattform beseitigt diese Probleme und ermöglicht es so Resellern, Systemhäusern, IT-Abteilungen sowie Service Providern effizient auf dem Outsourcing-Security-Markt zu agieren.

Die Clavister Security Service-Plattform (SSP) steht für das gesamte Clavister-Produktportfolio von Security-Gateways, UTM-Appliance- sowie Management Systeme und den damit zusammenhängenden Sicherheits-Services. Diese Lösung, kombiniert mit den Clavister Lifecycle-Systemen FineTune, PinPoint, und Insight setzt einen neuen Standard für Managed Security Services, da sich einerseits die Total Cost of Ownership (TCO) auf ein Minimum reduzieren lässt und andererseits ein rascher Return of Invest (ROI) erreichen lässt: sowohl für KMUs, die ihre Security an externe Dienstleister auslagern, als auch für Konzerne, die über interne IT-Serviceabteilungen verfügen und Service Provider, die ihren Kunden wiederum Sicherheitsdienstleistungen anbieten wollen. FineTune und PinPoint werden von Clavister kostenlos angeboten, wodurch Managed Security Service Provider im Gegensatz von herkömmlichen Lösungen massiv Geld sparen können. Die Hardware-Basis in den Zentralen bilden dabei UTM-Appliance-Systeme der 4000er-oder 3000er-Systemreihen. Zur Anbindung von Niederlassungen kommt beispielsweise die SG10-Serie zum Einsatz. Die SG10-Serie garantiert Managed Security Service Providern eine optimale und sichere Anbindung von kleinen Firmen oder Außenstellen. Damit werden Kompromisslösungen vermieden, die Service Provider in der Vergangenheit dazu gezwungen hatten sich zwischen Standardprodukten mit unzureichenden Funktionen oder teuren Lösungen mit unnötig vielen Features zu entscheiden. Die SG10-Serie bietet darüber hinaus noch weitere Vorteile: Beispielsweise kann eine Antivirus Scan-Engine und eine Supportfunktion für Clavisters InSight Reporting- und Logfile-Analyse-System genutzt werden. Ebenso enthält die Serie eine Web Content Filtering-Funktion sowie ein Intrusion Detection und Prevention (IDP/IPS) System.

Die Lösung ermöglicht einen schnellen und kosteneffizienten Einsatz der Managed Security Services (MSS), beispielsweise in den Bereichen:

- Managed VPN
- Managed Wireless Network Protection
- Managed Firewalling
- Managed Intrusion Detection and Prevention (IDP)
- Managed Antivirus Protection
- Managed Content Filtering
- Managed Web-Use Reporting
- Managed Regulatory Compliance Reporting

Die Clavister SSP zeichnet sich durch die Fähigkeit aus, sich an das Wachstum der Unternehmen anpassen zu können (Clavister xPansion Lines). Hierzu wurde die Lösung mit Feinabstimmungsmechanismen und hochgradig skalierbaren Funktionen ausgestattet, die es jedem Betreiber ermöglichen, diese an seine individuellen Leistungs- und Funktionsanforderungen nahtlos anzupassen. Die Tatsache, dass sowohl der Clavister SSP als auch das Customer Premise Security Gateway (CPE) dasselbe hoch skalierbare Betriebssystem Clavister CorePlus™ verwenden, macht jegliche Kompromisse zwischen maximalem Service, Verfügbarkeit, Funktionalität, Steuerbarkeit, TCO sowie Kapitalinvestitionen hinfällig.

Zentrales Remote Management

Mit FineTune steht den Anbietern von Managed Security Services ein modernes, graphisch orientiertes Management-System (GUI) zur Verfügung, das die zentrale Verwaltung einer Vielzahl von Clavister Security-Gateways aus einer benutzerfreundlichen GUI-Umgebung heraus ermöglicht. Über dieses Management-System ist die Remote-Verwaltung aller Clavister-Devices inklusive deren Konfiguration, Real Time-Monitoring sowie -Logging, Revisionskontrolle und Firmware Upgrades möglich und wird via 128-Bit-Verschlüsselung und Authentifizierungsmechanismen effektiv geschützt.

Sicherheitsprozesse in Echtzeit überwachen

Mit Clavister-PinPoint™ ist ein neues Tool verfügbar, mit dem Sicherheitsprozesse in Echtzeit überwacht werden können. Dieses ermöglicht Security Managern über eine intuitiv zu bedienende Oberfläche einen grafischen Überblick u.a. über Surfgewohnheiten, Resultate von Virus- oder Malware-Scans, Einbruchsversuche in das Netzwerk oder VoIP-Statistiken. Vergleichbar mit einem Flugzeug-Cockpit, können die „Piloten" von PinPoint essenzielle Daten (Mission Critical) von weniger wichtigen (Non-Critical) unterscheiden und anzeigen lassen. Clavister ist der erste Hersteller, der eine einfach zu bedienende Applikation auf den Markt bringt, die Security-abhängige Vorfälle in Echtzeit visualisiert.

Virtual Security Gateway – Sicherheit für virtuelle Umgebungen

Mit dem Clavister Virtual Security Gateway für VMware lassen sich virtuelle Systeme wirksam vor Hacker-Attacken und Malware schützen, da die Gateways über alle Funktionen der Hardware Appliance Security Gateways verfügen, inklusive aller UTM-Services. Darüber hinaus schützen Sie die Kommunikation der virtuellen Systeme untereinander durch den Einsatz von VPN-Verschlüsselung. Auch hinsichtlich der Security Policies müssen keine Einschränkungen gemacht werden, da sich die einmal definierten Policies auch auf die virtuellen Maschinen anwenden lassen. Das Virtual Security Gateway eignet sich auch zum Einsatz in Datencentern. Weitere Vorteile sind: Einfache Wartung, hohe Skalierbarkeit, virtuelle Systeme (OOBs), IDS und Auditing.

Auch wenn die Firmen noch zögern, insgesamt mehren sich die Anzeichen dafür, dass sich der MSS-Markt in einem Aufschwung befindet. Das zeigt die Umsatzentwicklung der europäischen Security-Outsourcing-Anbieter: Die Analysten von Gartner bescheinigen diesen eine durchschnittliche jährliche Wachstumsrate von 14,9 Prozent.

CLAVISTER™

Clavister Deutschland
Bülowstrasse 20 · 22763 Hamburg
Tel.: +49 40 411259-0
Fax: +49 40 411259-19
E-Mail: info@clavister.de
www.clavister.de



Systems 2008
Halle B3/
Stand 505

Vereinbaren Sie unter folgendem Link einen Termin mit uns auf der Systems: www.clavister.com/offers/systems08/ und sichern Sie sich so eine kostenlose Vollversion des neuen Clavister Virtual Security Gateway für VMware.

Den Zustand von Computern, die das Installieren oder wenigstens Ausführen von extern aufgespielter Software erlauben, können NAC-Systeme mithilfe von Client-Komponenten ermitteln. Auf dem Endgerät installierte Software kann Änderungen dort permanent protokollieren. Dabei müssen nicht immer spezielle NAC-„Agenten“ im Spiel sein. Auch NAC-kompatible Sicherheitspakete für PCs, neuere Betriebssysteme selbst oder Patch-Managementsysteme können die Rolle des Informationslieferanten über den Rechnerzustand übernehmen.

Wo nichts ohne Zustimmung installiert werden kann oder darf, lässt sich ein Gerät vielleicht auf eine Website leiten, die es dann mithilfe von ActiveX- oder Java-Applets überprüft. Im Zweifelsfall muss man den Anwender einbeziehen – beispielsweise, indem man ihm einen erweiterten Zugang nur gewährt, wenn er bestimmte Softwarepakete selbst herunterlädt und installiert. Manche NAC-Systeme starten sogar Vulnerability-Scans auf Geräten, die sich mit dem Netz verbinden.

Standards in Sicht

Die Durchsetzung der Richtlinien für die Zugriffsrechte im Netz sowie die Zuordnung zu einem bestimmten Subnetz oder VLAN, die das NAC-System aus den für ein Gerät geltenden generellen Policies und seinem Zustand ableitet, können im Netz unterschiedliche Systeme übernehmen: Infrastrukturkomponenten wie Switches, spezielle Appliances mit Router- und Switch-Funktionen oder Server-Softwareprodukte. Die zuletzt genannte Lösung präsentiert sich dabei gern selbst als die flexibelste, weil sie keine Bindung an einen Switch- und Komponentenhersteller mit sich bringt und auch in heterogenen Netzen gut funktioniert. Allerdings lässt sich inzwischen beobachten, dass die großen Infrastrukturanbieter mit ihren NAC-Lösungen aufeinander zugehen und diese zueinander kompatibel gestalten. Eine besondere Rolle spielt dabei die von der Trusted Computing Group gegründete Arbeitsgruppe „Trusted Network Connect“, die Standards schaffen will. Auch in Deutschland, etwa an der FH Gelsenkirchen und FH Hannover im Rahmen des Projekts tnac, arbeitet man an Lösungen für mehr Interoperabilität und Kompatibilität.

NAC-Appliances können „inline“ wie eine Firewall vor dem gesamten zu schützenden Netz arbeiten oder als „Out-of-Band“-Einheiten, die andere Netzwerkkomponenten steuern. Nicht jedes NAC-System gibt sich mit der „Pre-Connect-Kontrolle“ zufrieden – manche arbeiten in einer gewissen Analogie zu Intrusion-Detection-Systemen als „Post-Connect-NAC“ und prüfen permanent, ob ein Computer im Netz verdächtig agiert. Sinnvoll kann auch eine passive Überwachung des Address Resolution Protocols (ARP) sein. Computer, die Schutzmechanismen auf 802.1X- oder DHCP-Ebene entgangen sein könnten, müssten zumindest dort durch Aktivität auffallen.

Die letzte NAC-Komponente, die Durchsetzung der Richtlinien auf den PCs selbst, übernehmen wiederum die dort installierten Clients – sofern dem Anwender die entsprechenden Reparaturen nicht einfach im Remediation- oder Quarantäne-Segment aufgezwungen werden können. Die Clients können helfen, bei Richtlinienabweichungen Software neu aufzuspielen, bestehende Programme zu aktualisieren oder unerwünschte Programme zu löschen.

Betrachtet man die ganze Bandbreite von NAC-Systemen, reicht diese von der einfachen Abfrage der Netzkomponenten via SNMP bis hin zu den erwähnten, umfassend in Netzwerkinfrastrukturen integrierten Lösungen. Dabei kommt immer wieder der Vorwurf auf, keines dieser Systeme sei perfekt: Client-Komponenten etwa lassen sich fälschen, und DHCP-gestützte Ansätze, die Geräte über Adresszuweisungen steuern, scheitern manchmal schon daran, dass sich ein Computer mit einer fest vorgegebenen IP-Adresse anmeldet. Solche Kritik geht aber von falschen Prämissen aus. NAC richtet sich nicht primär gegen ausgewiesene Industriespione, sondern gegen Gefahren, die aus den Nebenwirkungen der heutigen Mobilität entstehen. Diese Risiken reduzieren die existierenden Systeme bereits recht gut.

Die Zahl und die Vielfalt der mobilen Geräte – von Notebooks und Tablet PCs bis hin zu Handys, PDAs, Smartphones und verschiedenen portablen Speichermedien – in einer unternehmensweiten Umgebung sowie die vielen unterschiedlichen Nutzer und Wege des Zugangs zu den Daten machten es häufig erforderlich, neben einem NAC zusätzliche Sicherheitsmaßnahmen einzuführen. Dazu gehört die Verschlüsselung von Festplatten, wobei sich der Nutzer mit einem Boot-Kennwort an seinem Gerät authentifizieren muss. Erst dann startet das Betriebssystem und generiert die Schlüssel, sodass die Daten bei Anforderung ent- und bei der Speicherung wieder verschlüsselt werden können. Diese Methode kann aber nicht alle heute vorhandenen mobilen Devices schützen, außerdem gehen damit weitere Nachteile für Administratoren einher: Sie müssen zusätzlich Kennwörter in einem Modus verwalten, in dem noch kein Netzwerk vorhanden ist.

Außerdem sind Prozesse wie das Aufspielen von Patches für Betriebssysteme oder Anwendungen komplizierter, denn diese können nicht wie im Unternehmen üblich automatisiert über Nacht ablaufen. Bei Reboot-Vorgängen hakt es nämlich aufgrund des einzugebenden Kennworts. Doch gibt es auch intelligente Verschlüsselungslösungen, die mithilfe von Policies arbeiten. Über das Regelwerk lässt sich differenziert bestimmen, welche Daten für welche Nutzer zugänglich sind: Dafür lassen sich Dateitypen (etwa alle doc-Dateien) bestimmen, Zugriffe pro Nutzer festlegen, ganze Anwendungen auf eine bestimmte Art schützen oder der Umgang mit bestimmten Geräten angeben. Schließlich kann der Sicherheitsverantwortliche auch Systemdaten wie lokale oder Domänen-Zugangsdaten, Paging-Dateien oder temporäre Dateien über Regeln verschlüsseln.

Bettina Weßelmann
Die Autorin arbeitet als freie Journalistin in München.

OPEN SOURCE NAC

Lösung	Webadresse
FH Gelsenkirchen	www.internet-sicherheit.de/forschung/aktuelle-projekte/tnac
Free NAC	www.freenac.net/de
Hupnet	hupnet.sourceforge.net/
Netreg	www.net.cmu.edu/netreg
Packet Fence	packetfence.org/
Rings	sourceforge.net/projects/rings
Ungoliant	ungoliant.sourceforge.net/

Ausgelagert

Managed Security Services – Sicherheit aus fremder Hand

Viele kleine Unternehmen haben weder das Know-how noch die personellen Ressourcen, um die steigenden Anforderungen an die IT-Security umzusetzen – Grund genug, über Managed Security Services nachzudenken.

Besonders kleine und mittlere Unternehmen sind mit Aufbau und Pflege einer effektiven IT-Sicherheitstechnik oft überfordert, da es ihnen häufig an personellen Ressourcen, aber auch an Spezialwissen fehlt. In den letzten Jahren haben sich im Bereich IT-Sicherheit zahlreiche neue Dienstleistungen entwickelt. Die sogenannten Managed Security Services reichen von der Konfiguration, Wartung und Aktualisierung von einzelnen Sicherheitssystemen bis hin zur vollständigen Übernahme von Sicherheitsaufgaben durch den Dienstleister.

Als Markttreiber gelten die zunehmenden und ständig neuen Bedrohungen, Wirtschaftlichkeitsbetrachtungen und das Erfordernis, gesetzliche Anforderungen zu erfüllen. Auch wächst das Bewusstsein für potenzielle Schäden. Trotzdem zögern besonders kleine und mittlere Unternehmen noch damit, einzelne Sicherheitsbausteine auszulagern.

Nach der Studie IT-Security 2007, die CMP Weka auf dem Kongress „Live Security“ in Berlin vorgestellt hat, nutzen nur 25 Prozent der Befragten Managed Security Services in ihren Unternehmen. Rund 71 Prozent antworteten auf die Frage „Hat Ihr Unternehmen einzelne IT-Sicherheitsanwendungen an externe Dienstleister vergeben?“, schlicht mit „Nein“.

Ein großer Vorteil der Managed Security Services ist, dass die darauf spezialisierten Dienstleister sich die besten IT-Security-Technologien sowie die dazugehörigen Experten leisten und diese Kosten auf alle Kunden verteilen können, die sich damit auf ihr eigenes Kerngeschäft konzentrieren können. Diensteanbieter betonen darüber hinaus die Vorteile der Kostenreduzierung und -kontrolle für den Kunden, die Erhöhung des Sicherheitsniveaus bei einem Service rund um die Uhr, automatische System-Updates, eine Reduzierung von Administrations- und Wartungsaufwand sowie die Entlastung der internen Ressourcen.

Dienstleister auf dem neuesten Stand

Es gibt eine Vielzahl von Anbietern: Carrier, Application Service Provider, Outsourcer wie IBM oder HP und Diensteanbieter wie Symantec oder Kaspersky. Alle haben sich auf unterschiedliche Bausteine spezialisiert. Eine große Begriffsvielfalt für den ASP-Markt insgesamt sieht eco, der Verband der deutschen Internetwirtschaft. Da heißt es nicht mehr wie früher einfach Application Service Providing (ASP), sondern Software as a Service (SaaS), Web-based Services oder Managed Services, obwohl das Problem das gleiche geblieben sei.

Aber eine klare Abgrenzung der Dienstleister und ihrer Angebote wird dadurch schwierig, so eco, zumal jeder Anbieter seinen eigenen Schwerpunkt in den Vordergrund stellt.

Großer Leidensdruck bei E-Mail-Security

Im Bereich E-Mail ist Handlungsbedarf besonders angesagt, sonst wird dieser Kommunikationsweg für Unternehmen über kurz oder lang unbrauchbar. Entsprechend des großen Leidensdrucks tummeln sich hier zahlreiche Anbieter wie Kaspersky, Eleven, Symantec oder Messagelabs, die die ein- sowie ausgehende E-Mail-Kommunikation des Kunden zunächst auf eigene Server umleiten, dort prüfen und bereinigt von Schadsoftware und Spam zum Auftraggeber zurückliefern.

Damit wehren die Dienstleister die Bedrohung der Mail-Infrastruktur des Auftraggebers ab und können potenziell die geschäftsrelevante E-Mail-

ANBIETER VON MANAGED SECURITY SERVICES (AUSWAHL)

Anbieter	Webadresse
Antispameurope	www.antispameurope.de
BT Global Services	www.btglobalservices.com
Eco, Verband der deutschen Internetwirtschaft	www.eco.de
Eleven	www.eleven.de
Experton Group	www.experton-group.de
Forrester Research	www.forrester.com
Getronics	www.getronics.com/de
IBM	www.ibm.com/services/security
Integralis Deutschland	www.integralis.de
Internet Security Systems	www.iss.net
Kaspersky Lab	www.kaspersky.de
Message Labs	www.messagelabs.com
Secure Works	www.secureworks.com
Solutionary	www.solutionary.com
Symantec	www.symantec.de
Unisys Deutschland	www.unisys.de
Verisign Deutschland	www.verisign.de

Kommunikation auch in Spitzenlastzeiten sicherstellen. Gefährliche E-Mails erreichen die unternehmenseigene IT-Infrastruktur erst gar nicht.

Selbstgestrickt war einmal

Alle Anbieter versprechen eine einfache Konfiguration durch eine Änderung des Mailserver-Eintrags im Domain Name System (DNS). Eleven spricht zum Beispiel von einer Konfiguration binnen zehn Minuten. Auch eine rechtskonforme Archivierung ist möglich. Darüber hinaus verbessert sich die Qualität der Spam-Filterung durch eine Auslagerung, da der Dienstleister eine wesentlich größere E-Mail-Menge zu Analysezwecken zur Verfügung hat und dadurch ganz andere Zusammenhänge herstellen kann.

„Managed Services, deren Flexibilität sowie die internetweite Sicht bieten Vorteile, die einzelne Appliances nicht erreichen können“, führte Alexander Peters von MessageLabs auf einem Konferenzvortrag aus. Er erwartet, dass sich der E-Mail-Security-Markt von reinen Software-Lösungen hin zu Managed Services entwickeln wird, wodurch interne Lösungen „Marke Eigenbau“ künftig der Vergangenheit angehören.

Wichtig ist jedoch, dass jedes Unternehmen den für sich und seine Bedürfnisse passenden Dienstleister findet. Einen großen Stellenwert hat in diesem Zusammenhang die Definition (und Einhaltung) von Service Level Agreements, der nach der Meinung der Experton Group oft nicht genügend Beachtung geschenkt wird. Die Folge sind Missverständnisse zwischen Dienstleister und Auftraggeber.

Auch sollte das Unternehmen vor dem Outsourcing das Gefahrenpotenzial bewerten und einschätzen, wie hoch die Abhängigkeit der Business-Prozesse von der IT-Infrastruktur ist. Welche Systeme müssen beispielsweise für das Aufrechterhalten der Produktion verfügbar sein?

Und Security Policies, grundlegende Sicherheits- und Verhaltensrichtlinien, sollte es geben – hier besteht großer Nachholbedarf. Nur knapp 19 Prozent der Unternehmen besitzen eine komplette Beschreibung, die anderen begnügen sich mit einer vagen schriftlichen Aufzeichnung (26 %) oder informellen Regelungen (rund 25 %). Und die sind nur bei wenigen Mitarbeitern bekannt: Nur 25 Prozent der online Befragten gaben an, dass wirklich alle Mitarbeiter die Sicherheitsrichtlinien auch kennen. Das stellten die Autoren der bereits zitierten Studie IT Security 2007 fest.

Outsourcing kann nur erfolgreich sein, wenn ein Unternehmen im Vorfeld geklärt hat, was der Dienstleister besser kann als die eigene IT. Geht es lediglich darum, nicht gelöste Probleme an Dritte weiterzugeben, bekommt der Auftraggeber nach der Erfahrung von Experton in 75 Prozent der Fälle die Probleme zurück, aber nicht die Lösungen.

Darüber hinaus sollte ein Unternehmen auf einen ständigen Zugriff auf die Informationen achten und genügend internes Know-how behalten, um überhaupt beurteilen zu können, inwieweit der Anbieter die vereinbarte Leistung erbracht hat.

Insgesamt gilt es, die Balance zu halten zwischen sinnvollem Outsourcing und Teil-Outsourcing, ohne in eine so kritische Abhängigkeit vom Dienstleister zu geraten, dass es kein Zurück im Rahmen eines „Insourcing“ mehr geben kann. In besagter Studie hatte nur knapp die Hälfte der bereits outsourcenden Unternehmen ihre Verträge so gestaltet, dass sie im Zweifelsfall die Auftragsvergabe zurückabwickeln können.

Barbara Lange
ist IT-Journalistin und Inhaberin des Redaktionsbüros kurz&einfach in Lengede.

In iX extra 12/2008:

Storage – Backup-Software im Unternehmen

Dass die Unbeliebtheit von Datensicherung mit ihrer Vernachlässigung korreliert, ist eine weithin bekannte Tatsache. Dennoch bleibt diese Erkenntnis viel zu oft folgenlos – bis das sprichwörtliche Kind in den Brunnen gefallen ist. Dabei haben sich die Anbieter von Backup-Software in den letzten Jahren wirklich Mühe gegeben, ihren Lösungen das Graue-Maus-Image zu nehmen. Es geht um Begrifflichkeiten wie Snapshots, Clones, Deduplizierung und CDP. Was dahintersteckt und wer es anbietet, im nächsten iX extra.

Erscheinungstermin: 20.11.08

DIE WEITEREN IX EXTRAS:

Ausgabe		Thema	Erscheinungstermin
01/09	Networking	Hosting-Provider – Kosten-Service-Analyse	18.12.08
02/09	Embedded Systems	Industrie-PCs und ihre Betriebssysteme	22.01.09
03/09	IT-Security	Identitätsmanagement in heterogenen Netzen	19.02.09